Jurnal Diplomasi Pertahanan,
Volume 8, Nomor 2, 2022 E-ISSN 2746-8496

CYBER WARFARE AS PART OF RUSSIA AND UKRAINE CONFLICT

Ujang Priyono
Master Student of Defense Diplomacy, Indonesia Defense University
Email: masterjaunk@gmail.com

Abstract

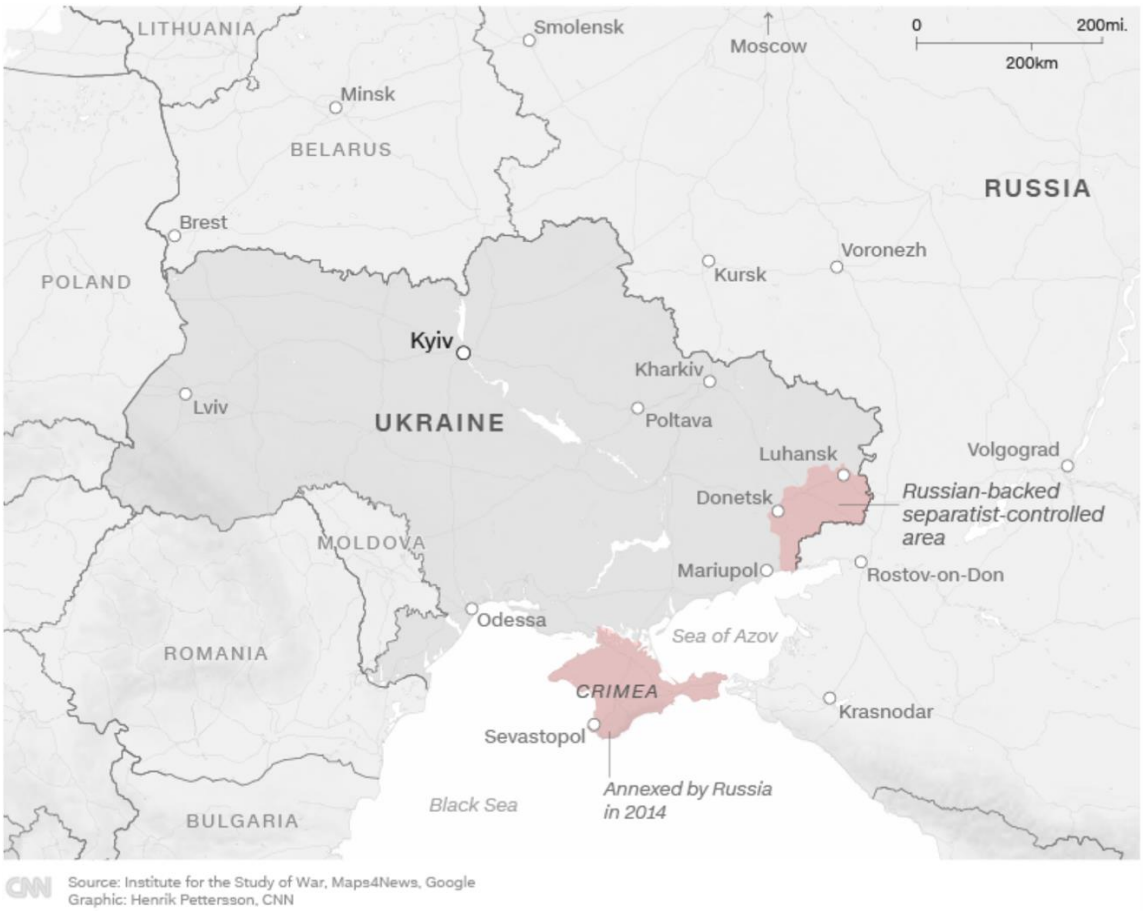
Russia and Ukraine have had tense relations since 2014, with violence erupting as a result. Cyber attacks have become an integral aspect of this conflict, in addition to the border issue and the separatist movement in Ukraine. Tensions between the two countries grew in 2021, and a significant cyber attack on the Ukrainian government website occurred in early 2022. Because the Ukrainian government claims that Russia was the brains behind the cyber assault, it has exacerbated the dispute between the two countries. Based on the timing of the wars and cyber attacks related to Ukraine, the goal of this study is to examine the relationship between cyber assaults and the political policies of the two countries toward the conflicts that occur. It also describe about the cyberspace dilemmas related to find the evidence of the real actors of cyber attacks.

Keywords: *Russia, Ukraine, Cyber Attack, Cyber Incident, conflict*

1. Introduction

In 1991, Ukraine declared independence from the Soviet Union. Ukraine was close to the heart of Russia until recently, compared to other parts of the Soviet Union. Even so, Russians consider Ukraine to be a part of their culture. The relationship, however, is far from equal. Russia has been waging war against Ukraine for many years. Tensions between Russia and Ukraine flared in March 2014, when Russian troops seized control of Ukraine's Crimea region and annexed the peninsula after Crimeans opted to join the Russian Federation in a disputed local referendum. The rights of Russian people and Russian-speakers in Crimea and southeastern Ukraine must be protected, according to Russian President Vladimir Putin.

Since April 2014, the confrontation between Russian-backed separatists and Ukrainian military forces has claimed the lives of 10,300 people and left 24,000 others injured. Russia, on the other hand, maintains its denial that it is involved in the separatist movement in Ukraine, despite the fact that it continues to establish military outposts along the border. This situation has eventually compelled NATO members, the United States and Europe, to seek a diplomatic solution between the two countries.



Ukraine has been a frequent victim of cyber attacks since the conflict with Russia began. Attacks on Ukrainian power companies were the most common cyberattacks, with more than 225,000 people losing power across Ukraine in December 2015, and portions of Kiev experiencing another power outage in December 2016 following a similar attack. Ukraine's government and business computer systems were not immune to cyber attacks. In June 2017, the NotPetya cyber attack, which was linked to Russia, spread to computer systems all over the world, causing billions of dollars in losses.

According to Bloomberg, Ukraine had its deadliest cyber strike in four years on January 14, 2022, when nearly 70 of its government entities were targeted by enormous cyber attacks. According to Ukrainian authorities, the hack did not result in any significant data leaks, but investigators are still working on the case and gathering evidence. Based on these circumstances, the purpose of this research is to determine whether there is a link between the cyber assaults in Ukraine and the conflict between Russia and Ukraine. The next section will discuss the timing of cyber attacks and the growth of tensions between Russia and Ukraine in order to address this question.

2. Literature review

2.1. The Conflict Timeline of Russia and Ukraine

As previously noted, the crisis between Russia and Ukraine has drawn the United States into a direct role in its density. The two countries have had several bilateral encounters, both at the foreign ministry level and between the two great powers' leaders. However, no deal has yet been achieved between the two warring countries that will lead to peace. President Joe Biden had previously stated that if Russia continued to intervene against Ukraine, it would face severe economic consequences. Biden also stated that if the situation intensified, he would send defense assistance to Ukraine. Biden, on the other hand, stated that he would not build troops in Ukraine because the country is not a NATO member.

On the other hand, Ukraine's president continues to accuse Russia of bolstering its military force along the country's border, which is a source of tension between the two nations. Meanwhile, Russia has stationed around 120,000 troops in Ukraine's territory, as well as short-range ballistic missiles, tanks, and other heavy military equipment near the Ukrainian line. This demonstrates that, in terms of the Ukraine issue, diplomatic ties between the US and Russia are at an all-time low. More information can be found in the table below:

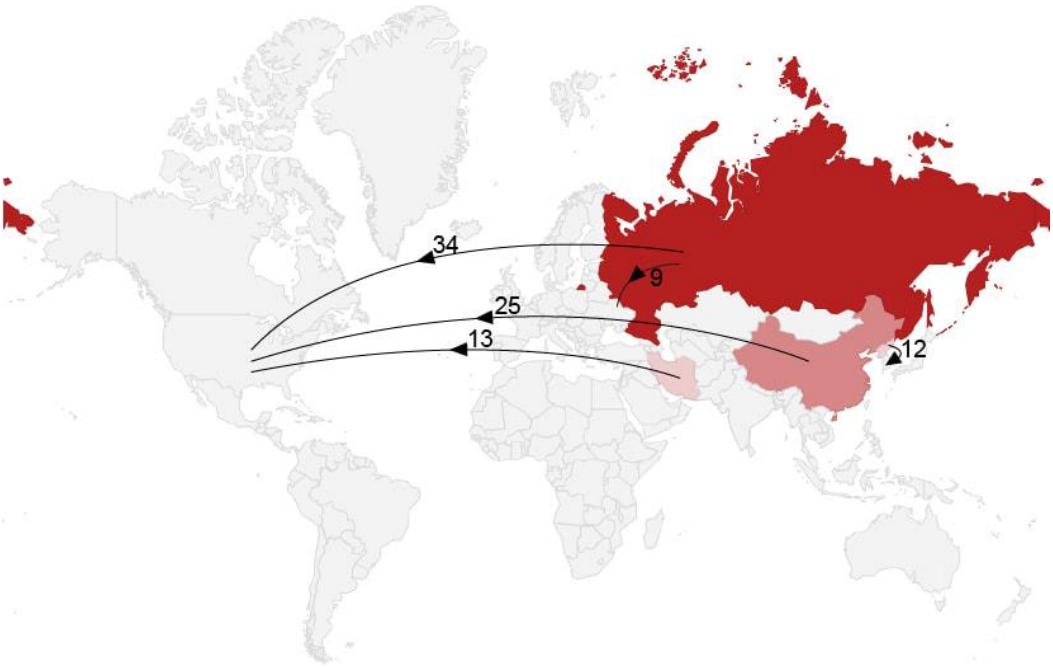
Date	Events
March 2014	The taken of Crimea aggravated US-Russian relations. Russia's unilateral action provoked the United States to impose economic sanctions on the country.
April 2014	A conflict erupted between separatists backed by Russia and the Ukrainian Army.
2015	France and Germany attempted, but failed, to persuade Russia and Ukraine to sign a political agreement.
2015 - 2020	In eastern Ukraine, deadly battles between Ukrainian forces and pro-Russian separatists were common. The clashes between the two sides have resulted in the deaths of over 13,000 individuals and the displacement of 1.5 million people.
February 2021	The United States accuses Russia of obstructing a peaceful resolution to the dispute. The taken of Crimea, according to Biden, The United States will "never" accept it.
March 2021	President of the European Union Charles Michel announces that the EU will retain sanctions on Russia as long as Putin continues to encourage pro-Russian separatists.
April 2021	Ukraine has expressed its displeasure with the recent uptick of violence. Moscow said it is concerned about a "full-fledged conflict" in the region.
June 2021	The President of Ukraine has appealed to the country's Western friends to intervene.
August 2021	Ukraine has the steadfast support of President Joe Biden.
November 2021	Ukraine's authorities, Russia claims, are attempting to pull Moscow into the conflict in eastern Ukraine. The announcement comes as violence between

	government forces and rebels in the breakaway province has intensified.
December 2021	Biden warned Putin in a teleconference that if military escalation occurs, the US will respond with harsh economic and other consequences.

2.2. The Cyber Attacks From Russian Hacker

Russia launched cyber attacks against 19 countries, according to an article written by Joe Robinson, a data privacy and cyber security expert, this attacks resulting in 75 incidents between 2009 and 2019. The US and other European nations were the primary targets of these assaults, with Ukraine ranking among the most frequently attacked by Russia in a short period of time, with nine attacks between 2017 and 2019.

	Source	Target	Attacks
1.	Russia	USA	34
2.	China	USA	25
3.	Iran	USA	13
4.	North Korea	South Korea	12
5.	Russia	Ukraine	9



According to statistics supplied by the Center for Strategic and International Studies (CSIS) on key cyber incidents dating back to 2006, there have been a slew of occurrences involving Russia as the accused perpetrator.

Date	**Cyber Attack**
Dec-21	A ransomware attack on Australian power firm CS energy was blamed on a Russian gang. This announcement came after Australian news outlets blamed the attack on Chinese government hackers.
Nov-21	Personal information of roughly 3,500 people, including government officials, journalists, and human rights advocates, was targeted by a Russian-speaking organization. To obtain access to private email accounts and financial information, the group utilized malware on Android and Windows devices.
Oct-21	The Russian Foreign Intelligence Service (SVR) has initiated a campaign aimed at resellers and other technological service providers who customize, deploy, and manage cloud services, according to an American corporation.
Sep-21	The EU officially condemned Russia for its role in the 'Ghostwriter' cyberattack, which targeted numerous EU member nations' elections and political processes. Russian hackers have been hacking government officials' social media accounts and news websites since 2017, with the purpose of instilling doubt in US and NATO military.
Sep-21	Ghaleb Alaumary was sentenced to more than 11 years in jail by the US Department of Justice for assisting North Korean cybercriminals in money laundering. ATM cash-out operations, cyber-enabled bank robberies, and business email compromise (BEC) schemes were among the services he provided. In the United States and the United Kingdom, these attacks targeted banks, professional soccer clubs, and other unspecified businesses.
Sep-21	a cyberattack on the United Nations targeted users on the UN network in order to obtain long-term intelligence. The hacker gained access to their networks by purchasing stolen user credentials on the dark web.
Sep-21	A series of cyberattacks against private and public IT systems, according to the Norwegian government, were carried out by criminal actors supported by and operating out of China. According to their investigation into the attacks, the perpetrators tried to obtain classified material about Norway's national defense and security intelligence.
Aug-21	a cyber-espionage outfit associated to one of Russia's secret services attempted spear-fishing attacks on the Slovak government.

Aug-21	In order to coordinate anti-Kremlin voting in the parliamentary elections next month, Russia targeted and blocked information on a smart voting software built by Kremlin foe Alexei Navalny and his friends.
Jul-21	The Russian defense ministry said it was the victim of a DDoS attack that forced the shutdown of its website, claiming the attack originated outside the Russian Federation.
Jul-21	Russian hackers took advantage of a flaw in Kaseya's virtual systems/server administrator (VSA) software to launch a ransomware assault on the company's network. Around 1,500 small and midsized firms were hacked, and the criminals demanded $70 million in payment.
Jul-21	The Ukrainian Ministry of Defense stated that Russian hackers hacked its naval forces' website and published false reports concerning the multinational Sea Breeze-2021 military exercises.
Jun-21	DDoS assaults were allegedly launched against Vladimir Putin's annual phone-in event, according to Russia.
Jun-21	Hackers affiliated to Russia's Foreign Intelligence Service put malicious software on a Microsoft system, giving them access to accounts and contacts. The majority of the consumers targeted were based in the United States and worked for IT firms or the government.
Jun-21	From 2019 through 2021, the Russian GRU tried a series of brute force access attacks against hundreds of government and private sector targets around the world, targeting firms using Microsoft Office 365® cloud services, according to the US and British governments.
Jun-21	The tracking data of two NATO ships, the HMS Defender of the United Kingdom Royal Navy and the HNLMS Evertsen of the Royal Netherlands Navy, was allegedly fabricated off the coast of a Russian-controlled naval base in the Black Sea, according to the United States Naval Institute (USNI). The two vessels were positioned near the entrance to a key Russian naval base, according to the forged data.
Jun-21	More than 30 senior Polish officials, ministers and lawmakers from political parties, as well as several journalists, had their email accounts hacked, according to reports.
Jun-21	REvil, a Russian-linked hacking outfit, targeted Sol Oriens, a small government contractor that works for the Department of Energy on nuclear weapons issues.
Jun-21	In 2017, hackers working for Russian intelligence services are thought to have penetrated the internal network of the Netherlands police force. The attack happened as the country was investigating the downing of Malaysia Airlines Flight 17 (MH17) in 2014.

May-21	A ransomware attack hit JBS, the world's largest meat processing company, situated in Brazil. Facilities in the United States, Canada, and Australia were all shut down as a result of the attack. REvil, a Russian-speaking cybercrime outfit, was blamed for the attack.
May-21	The Health Service Executive, Ireland's national health service, was targeted by a ransomware attack (HSE). The HSE system was shut down by government officials after the attack was discovered. The attackers used the Conti ransomware-as-a-service (RaaS), which is said to be run by a cybercrime group based in Russia.
May-21	A ransomware attack was launched on the Colonial Pipeline, the country's major petroleum pipeline. The pipeline was shut off by the energy corporation, which later paid a $5 million ransom. DarkSide, a Russian-speaking hacking gang, is blamed for the attack.
May-21	A Russian defense business involved in designing nuclear submarines for the Russian navy was hacked by a Chinese hacking organization.
Apr-21	As tensions between the two countries increased in early 2021, Spearphishing cyberattacks were performed against Ukrainian government officials by Russian hackers.
Apr-21	In response to charges of Russian government-sponsored doping of Russian athletes, Swedish officials revealed that the Swedish Sports Confederation was hacked by Russian military intelligence in late 2017 and early 2018.
Mar-21	After breaking into the email system of the US State Department, suspected Russian hackers seized thousands of emails.
Mar-21	In the run-up to Germany's national elections, suspected Russian hackers sought to obtain access to the personal email accounts of German lawmakers.
Mar-21	Suspected Russian hackers briefly took control of the websites of Poland's National Atomic Energy Agency and the Ministry of Health in order to broadcast false alerts about a nonexistent radioactive threat, according to Polish security authorities.
Mar-21	In unconnected efforts in 2020, Russian and Chinese intelligence agents targeted the European Medications Agency, seizing material linked to COVID-19 vaccines and medicines.
Mar-21	Ukraine's State Security Service announced that it has foiled a large-scale attempt by Russian FSB hackers to obtain access to confidential government information.
Mar-21	Russian hackers targeted important Lithuanian officials in 2020, according to Lithuania's State Security Department, and used the country's IT infrastructure to launch assaults against organizations working on a COVID-19 vaccine.

Feb-21	Russian hackers gained access to a Ukrainian government file-sharing system and sought to spread harmful documents that would infect computers that downloaded them.
Feb-21	A multi-day distributed denial-of-service attack against the website of Ukraine's Security Service was revealed by Ukrainian officials as part of Russia's hybrid warfare activities in the country.
Feb-21	A Russian hacking outfit was behind a four-year assault against French IT companies, according to the French national cybersecurity agency.
Dec-20	Facebook discovered that two groups of Russians and one group of individuals associated with the French military were conducting dueling political information operations in Africa using phony Facebook accounts.
Dec-20	Russian hackers infiltrated the software supplier SolarWinds and exploited their access to monitor internal operations and exfiltrate data at over 200 businesses around the world, including various US government institutions.
Nov-20	Seven firms participating in COVID-19 vaccine research were targeted by one Russian and two North Korean hacking outfits.
Oct-20	A Russian cyber espionage operation hacked an undisclosed European government agency.
Oct-20	A Russian cyber gang accessed U.S. state and local government networks, as well as aviation networks, according to the FBI and CISA.
Oct-20	Attacks on Russian aerospace and defense businesses were carried out by a North Korean cyber outfit.
Oct-20	The National Cyber Security Centre of the United Kingdom discovered evidence that Russian military intelligence hackers were plotting a disruptive cyber strike on the 2020 Tokyo Olympics, which were eventually postponed.
Oct-20	Six Russian GRU officers were indicted by the US for their roles in hacking incidents such as the 2015 and 2016 attacks on Ukrainian critical infrastructure, the 2017 NotPetya ransomware epidemic, and election meddling in the 2017 French elections, among others.
Oct-20	Microsoft and the US Cyber Command worked together to take down a Russian botnet before of the election in the United States.
Oct-20	Chinese hackers are suspected of being behind a series of attacks on entities in Russia, India, Ukraine, Kazakhstan, Kyrgyzstan, and Malaysia, according to US government officials.

Sep-20	Government institutions in NATO member countries and NATO cooperating countries were attacked by Russian hackers. The phishing scheme infects target PCs with malware that installs a permanent backdoor, and the campaign uses NATO training material as bait.
Sep-20	Norway reported that it had successfully guarded against two cyberattacks that targeted the emails of many members and staff of the Norwegian parliament, as well as public employees in the Hedmark region. It eventually blamed the strike on Russia.
Aug-20	In preparation for operations on Ukraine's independence day, Ukrainian officials announced that a Russian hacking group had begun a phishing campaign. Russian hackers hacked into news sites and substituted authentic articles with false comments from military and political authorities in an attempt to undermine NATO among Polish, Lithuanian, and Latvian audiences..
Aug-20	Hackers linked to Russian intelligence attempted to steal information relating to the development of the COVID-19 vaccine, according to Canada, the United Kingdom, and the United States.
Jul-20	Norway reported that it had successfully guarded against two cyberattacks that targeted the emails of many members and staff of the Norwegian parliament, as well as public employees in the Hedmark region. It eventually blamed the strike on Russia.
Jul-20	The United Kingdom revealed that it believes Russia tried to sabotage its general election in 2019 by stealing and exposing information relating to the UK-US Free Trade Agreement.
Jul-20	According to media sources, the CIA was given permission to launch cyber operations against Iran, North Korea, Russia, and China by a presidential decision made in 2018. Disruption and information leakage were among the operations.
Jul-20	Trump acknowledged that he gave the go-ahead for a US Cyber Command operation in 2019 to take the Russian Internet Research Agency down.
May-20	Russian hackers linked to the GRU have been exploiting a weakness that might allow them to take remote control of US servers, according to the NSA.
May-20	German officials discovered that a Russian hacker outfit linked to the FSB had hacked into the networks of German energy, water, and electricity corporations through their suppliers.
Apr-20	Poland claims the Russian government is behind a series of cyber attacks on Poland's War Studies University, which are part of a disinformation effort aimed at sabotaging US-Polish relations.
Jan-20	A Russian hacking organization attacked a Ukrainian energy business where Hunter Biden was previously a board member and which has been

	widely mentioned in the impeachment process in the United States.
Dec-19	In a spear phishing attack, Russian government hackers targeted Ukrainian diplomats, government officials, military officers, law enforcement, journalists, and nonprofit organizations.

3. Research Methodology

The research methodologies used in this study are descriptive qualitative research methods. Qualitative research, according to Sugiono, is research in which the researcher is a primary instrument, data gathering methodologies are merged, and data analysis is inductive (Sugiono. 2010 : 9). Descriptive research, on the other hand, is a study that uses data to try to solve an issue. In descriptive research, the analysis process entails presenting, evaluating, and interpreting data (Narbuko & Ahmadi. 2015).

In this research, the author employed a narrative style and a literature review to illustrate the link between the Russia-Ukraine conflict and Russian cyber attacks on Ukraine. The author of this study is looking for a link between political events in the two countries and the cyber attacks that happened in 2020 to 2021.

4. Results and Discussion

4.1. The Correlation

We can see that there is a probable correlation between Ukraine's or the US's political policies and the date of cyber assaults in Ukraine in the table below, which, of course, includes the cyber attacks that recently transpired in 2022. According to the information we have, the purported Russian cyber attack primarily targeted government institutions and vital government data; there were no attacks on the general population or other public facilities.

Political Events		Cyber Attack Incidents	
Feb-21	Russia is accused by the US of hindering a peaceful end to the conflict. According to Biden, the United States will "never" accept the takeover of Crimea.	Feb-21	Russian hackers obtained access to a file-sharing system used by the Ukrainian government and attempted to circulate malicious documents that would infect computers that downloaded them.
		Feb-21	Ukrainian officials reported that Russia's hybrid warfare actions in the country included a multi-day distributed denial-of-service attack against the website of Ukraine's Security Service.
Mar-21	As long as Putin encourages pro-Russian separatists, EU President Charles Michel announces that the EU would maintain sanctions on Russia.	Mar-21	The State Security Service of Ukraine reported that it has thwarted a large-scale attempt by Russian FSB hackers to get access to sensitive government data.
Apr-21	Ukraine has voiced its dissatisfaction with the current increase in violence. Moscow expressed alarm about the region devolving into a "full-fledged battle."	Apr-21	Russian hackers attempted spearphishing attacks on Ukrainian government officials as tensions between the two countries grew in early 2021.
Jun-21	Ukraine's president has pleaded with the country's Western allies to help.		
		Jul-21	Russian hackers accessed Ukraine's naval forces' website and published fake news about the multinational Sea Breeze-2021 military exercises, according to the Ukrainian Ministry of Defense.

According to a statement from Ukraine's deputy secretary of state for national security and defense, the perpetrators of the cyber attack known as UNC1151 against Ukraine have ties to Belarusian intelligence. The UNC1151 is a cyber-espionage organization related to Belarus' special services. The group has a history of targeting Lithuania, Latvia, Poland, and Ukraine, as well as disseminating narratives critical of NATO's stance in Europe, according to Ukraine's cyber police commander. The dangerous virus used to encrypt some government systems looks a lot like the malware used by the ATP-29 hacking gang, which was involved in hacking the Democratic National Committee before the 2016 US presidential election. This organization is related to Russia's special intelligence agencies, and its goal is to commit cyber espionage by recruiting and exploiting insiders. After the cyber attack, messages were left on the Ukrainian website in three languages: Ukrainian, Russian, and Polish. They were referring to Volhynia and Eastern Galicia, where the Ukrainian Rebel Army carried out mass executions in Nazi-occupied Poland (UPA). It is still a source of disagreement between Poland and Ukraine.

4.2. The Dilemma

The cyber world, as we all know, has an element of anonymity. The most tragic cyber attack in history occurred in Estonia in 2007, when a series of massive cyber attacks were launched against Estonian government websites, including banks, parliament, newspapers, and broadcasters, on April 27, 2007, in response to the country's dispute with Russia over the relocation of the Bronze Soldier of Tallinn in Tallinn's war cemeteries, as well as an elaborate Soviet-era burial monument. The Estonian government was eager to point the finger at the Kremlin, accusing it of direct complicity in the strike at the time. However, when Estonia's defense minister stated that he had no evidence linking the cyberattack to the Kremlin, it was proven that the charges were not totally genuine. Russia has declared the claims "baseless," and neither NATO nor the European Commission specialists have been able to establish evidence of the Russian government's formal involvement. The best thing to do, as Estonia

advocated in the aftermath of the attack, is to improve cybersecurity protection and incident management.

So, while we conclude that there is a link between cyber assaults in Ukraine and the war between Russia and Ukraine based on this analysis, the perpetrators of the attacks must be legally confirmed. And because this is ineffective, it is preferable to invest in a strong cyber defense and reliable cyber resilience than than focusing all efforts on locating the true perpetrator.

5. Conclusion

We can draw some conclusions about the study's questions based on the research completed. In the context of the war between Russia and Ukraine, the cyber attack in Ukraine is highly helpful for Russia, which is currently under a lot of pressure from the US and NATO over the Ukrainian border issue, regardless of whether it was carried out on Russian government orders or not. Non-state actors or anyone acting on behalf of particular countries or groups can exploit cyberspace, which is extremely harmful for global security because it can be used by third parties to increase tensions between countries. It's tough to track down the players who carry out cyber assaults since most people who are victims of these attacks don't want to talk about it because it jeopardizes a country's or organization's security credibility.

To perform a more in-depth study with more diverse objects and involve technological research on the types of assaults and their attack media, it is important to conduct a more in-depth study with more diversified objects and involve technological research on the types of attacks and their attack medium. In addition, a research of the users' security awareness is required. Because, in the security chain theory, the weakest part of the chain is belong to human.

References

Baezner, M. (2018, Oct). *Cyber and Information warfare in the Ukrainian conflict.* Zurich: Center for Security Studies (CSS).

Brumfield, C. (2022, Jan 19). *Russia-linked cyberattacks on Ukraine: A timeline*. Retrieved from csoonline.com: https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html

CNBCTV18.com. (2021, Dec 09). *Timeline of US-Russia tensions amid Ukraine invasion fears*. Retrieved from cnbctv18.com: https://www.cnbctv18.com/politics/timeline-of-us-russia-tensions-amid-ukraine-invasion-fears-11757492.htm

CSIS. (2021). *Significant Cyber Incidents Since 2006.* Retrieved from csis-website-prod.s3.amazonaws.com: https://csis-website-prod.s3.amazonaws.com/s3fs-public/220104_Significant_Cyber_Events.pdf?dLSQUtb9qiFpttFl7FcBmA9IKZaNPUib

Chance, M., & Smith-Spark, L. (2022, Jan 22). *Tensions are high on Ukraine's border with Russia. Here's what you need to know*. Retrieved from edition.cnn.com: https://edition.cnn.com/2022/01/20/europe/ukraine-russia-tensions-explainer-cmd-intl/index.html

Frisby, J. (2020, June 02). *Cybersecurity Exposure Index (CEI) 2020*. Retrieved from passwordmanagers.co: https://passwordmanagers.co/cybersecurity-exposure-index/#global

Nardelli, A., Kuznetsov, V., & Choursina, K. (2022, Jan 14). *Cyberattack Hits Ukrainian Websites as Russia Tensions Mount*. Retrieved from bloomberg.com: https://www.bloomberg.com/news/articles/2022-01-14/several-ukraine-ministry-websites-struck-by-likely-cyberattack

Neuman, S. (2022, Jan 14). Ukraine is hit by a massive cyberattack that targeted government websites. Retrieved from npr.org: https://www.npr.org/2022/01/14/1073001754/ukraine-cyber-attack-government-websites-russia

O'Neill, P. (2022, Jan 21). *How a Russian cyberwar in Ukraine could ripple out globally*. Retrieved from technologyreview.com: https://www.technologyreview.com/2022/01/21/1043980/how-a-russian-cyberwar-in-ukraine-could-ripple-out-globally/

Polityuk, P. (2022, Jan 15). *EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack*. Retrieved from reuters.com: https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/

Robinson, J. (2021, Nov 21). *Cyberwarfare statistics: A decade of geopolitical attacks*. Retrieved from privacyaffairs.com: https://www.privacyaffairs.com/geopolitical-attacks/

Sanger, D. E. (2022, Jan 16). *Microsoft Warns of Destructive Cyberattack on Ukrainian Computer Networks*. Retrieved from nytimes.com: https://www.nytimes.com/2022/01/16/us/politics/microsoft-ukraine-cyberattack.html

Windrem, R. (2016, Dec 18). *Timeline: Ten Years of Russian Cyber Attacks on Other Nations*. Retrieved from nbcnews.com: https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111

Zoria, Y. (2022, Jan 14). *Ukrainian official sites under massive cyberattack with a Russian trace*. Retrieved from euromaidanpress.com: https://euromaidanpress.com/2022/01/14/ukraine-under-massive-cyberattack-with-a-russian-trace/

bbc.com. (2017, Jan 11). *Ukraine power cut 'was cyber-attack`*. Retrieved from bbc.com: https://www.bbc.com/news/technology-38573074

bbc.com. (2022, Jan 14). *Ukraine cyber-attack: Russia to blame for hack, says Kyiv*. Retrieved from bbc.com: https://www.bbc.com/news/world-europe-59992531

cfr.org. (2021). *Global Conflict Tracker*. Retrieved from cfr.org: https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

wikipedia. (n.d.). *2007 cyberattacks on Estonia*. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia